Attachment A

AFFIDAVIT OF FBI SPECIAL AGENT ROBBIE J. ROBERTSON IN SUPPORT OF A CRIMINAL COMPLAINT

I, Robbie J. Robertson, Special Agent of the Federal Bureau of Investigation ("FBI"), being duly sworn, hereby declare as follows:

AGENT BACKGROUND AND BASES FOR STATEMENTS

1. I am a Special Agent with the FBI assigned to investigate cyber-crime, and have been so employed since September 2017. My training included attending FBI new agent basic training during which I received instruction on various aspects of federal investigations. Since May 2019, I have been assigned to investigate high technology and cyber-crime and have been involved in investigations of alleged computer-related and intellectual property offenses, including computer intrusions, trafficking in counterfeit goods, wire fraud, internet extortion, and other criminal matters. As an FBI agent, I am authorized to investigate violations of United States law and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. Prior to my current position as a Special Agent with the FBI, I obtained a Bachelor of Science degree in Information Technology. During my career as a Special Agent of the FBI, I have received training and possess actual experience relating to federal criminal procedures and federal statutes. I have also received specialized training and instruction in the field of investigation in computer-related crimes. I have had the opportunity to conduct, coordinate, and participate in numerous investigations relating to computer-related crimes. I have participated in the execution of numerous search warrants and arrest warrants conducted by the FBI.

2. The statements contained in this affidavit are based, in part, on my training, years of investigative experience, and my personal participation in this investigation. The statements contained in this affidavit are sometimes based on information provided by other FBI Special

Agents, other government agencies, as well as information derived from interviews of victim companies.

3. Because this affidavit is submitted for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me that supports probable cause. This affidavit does not purport to set forth all of my knowledge of, or investigation into, this matter. I have summarized information, including information received from law enforcement agents and officers, documents, and records. I have set forth those facts that I believe are sufficient to support the issuance of the requested arrest warrant. I am not relying upon facts not set forth herein to support my conclusion.

4. I am one of the agents participating in the investigation of Shariq Hashme ("HASHME") for offenses relating to the unauthorized access and damage to computers belonging to Company A, a San Francisco, California-based data analysis company.

5. As part of that ongoing FBI investigation, I make this affidavit in support of an application by the United States of America for a complaint and arrest warrant for HASHME.

6. As set forth herein, there is probable cause to believe that HASHME knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and thereby caused loss to one or more persons during a one-year period affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

APPLICABLE STATUTES

7. Under Title 18, United States Code, Section 1030(a)(5)(A), it is unlawful for an individual to "knowingly cause[] the transmission of a program, information, code, or command,

and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." A protected computer is a computer that is used in or affecting interstate or foreign commerce. *See* 18 U.S.C. § 1030(e)(2)(B). The term "damage" means any impairment to the integrity or availability of data, a program, a system, or information. *See* 18 U.S.C. § 1030(e)(8).

8. Under Title 18, United States Code Sections 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I), the penalty for a violation of 18 U.S.C. § 1030(a)(5)(A) is a fine and imprisonment of not more than ten years if the offense caused (i) loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; (v) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or (vi) damage affecting 10 or more protected computers during any 1-year period.

FACTS SUPPORTING PROBABLE CAUSE

Summary

9. Beginning at least as early as on or about February 26, 2019, continuing through and including on or about July 11, 2019, Shariq HASHME repeatedly connected to and caused transmissions to Company A's internal payment database to surreptitiously alter its data and contents without authorization in order to divert at least approximately $40,000 in payments to accounts controlled by HASHME.

10. HASHME, who was employed as an engineer at Company A, is an individual that resided in 2019 in San Francisco, California before on or about April 18, 2019, and outside the United States after on or about that date. HASHME worked for Company A as an employee

then later as a non-employee contractor during this time.

Background of Investigation

11. Company A is a San Francisco, California-based data analysis company.

12. PayPal is a web-based financial services provider based in Mountain View, California.

13. On May 8, 2019, representatives of Company A contacted the San Francisco Division of the FBI to report a criminal cyber incident. According to representatives of the company, they discovered their internal payment database, contained in their back-end computer network infrastructure, had been compromised in late April 2019.

14. Company A advised that it paid its employees through PayPal and would at times issue "bonus" payments to its employees through PayPal using its internal payment database, which also listed employees' personally identifiable information, including work related e-mail account information. Company A utilized "1Password," a service that streamlines access to multiple protected enclaves through a singular password and username. In this instance, each engineer was given access to a 1Password account and all administrator-level tasks were executed under the same account. Furthermore, 1Password automatically populated user names and passwords in order to access Company A's back-end infrastructure. Access to the company's internal payment database and other internal infrastructure was restricted using 1Password. Company A advised that the 1Password credentials were shared through each engineer's individually-operated GitHub account.

15. Company A reported that during this cyber incident, an individual connected to its internal payment database and altered payments that were originally directed to legitimate employees to divert them to a PayPal account linked to "Bruno.Day.1988@outlook.com"

("Subject PayPal account"). Company A determined that this re-direction of payments to the Subject PayPal account occurred through transmissions to its internal payment database using the 1Password account. Based on an internal investigation conducted by Company A, the majority of the altered payments made to the Subject PayPal account were in the amount of $140.00 beginning on or about March 12, 2019 and ending on or about May 6, 2019. Over the course of this cyber incident, Company A advised that a total of approximately 100 payments were altered in the internal payment database and diverted to the Subject PayPal account, resulting in losses of at least approximately $14,000.

16. Company A provided the FBI with a suspicious IP address of 182.232.191.125, which connected to its internal payment database around the time of one of the intrusion incidents on April 30, 2019 at 13:39:53 UTC. IP addresses oftentimes are associated with a particular geographic area or region based on them falling within certain known IP address ranges. The aforementioned suspicious IP address was confirmed to be associated with the particular geographic area of ("geo-located") of Thailand using open source research conducted by the FBI.

17. Following the initial incident, Company A advised the FBI of another similar cyber incident in which an individual manipulated the internal payment database and altered approximately 30 additional $140.00 bonus payments to divert them to the Subject PayPal account; these payments were processed on or about May 6, 2019, resulting in losses of at least approximately $4,200. This similar incident took place after Company A took additional security measures in response to the initial incident. For example, known IP addresses were "white listed" or allowed to access internal infrastructure, while unknown IPs were restricted.

18. On July 16, 2019, Company A advised the FBI of yet another similar cyber

incident in which an individual manipulated the internal payment database and altered approximately $15,000 in bonus payments, this time to divert them to a PayPal account linked to "dragonball844@outlook.com." The incident occurred on June 20, 2019, but was not discovered until July 12, 2019. No IP addresses were available, due to new database configurations at Company A.

Identification of HASHME

19. The FBI obtained records from PayPal for the account registered to Bruno.Day.1988@outlook.com. In part, PayPal records provided the subscriber information, IP logs and transaction history for the account registered to Bruno.Day.1988@outlook.com. From February 26, 2019 to June 13, 2019, this PayPal account received more than 190 payments from Company A that totaled approximately $26,663. The subscriber information of the PayPal account included the following:

First Name: Bruno
Last Name: Day
DOB: [redacted]
Address: [redacted]
Telephone: [redacted]
Time Created: February 26, 2019, 20:04:39

20. The FBI also obtained records from PayPal for the account registered to dragonball844@outlook.com. In part, PayPal records provided the subscriber information, IP logs and transaction history for the accounts registered to dragonball844@outlook.com. From June 28, 2019 to July 11, 2019, this PayPal account received more than 70 payments from Company A that totaled approximately $13,190. The subscriber information of the PayPal accounts included the following:

First Name: [redacted]
Last Name: [redacted]

Email: dragonball844@outlook.com
Address: [redacted]
Telephone: [redacted]
Time Created: June 24, 2019, 6:47:25

21. PayPal records also provided a "confirmed" cellular phone number for both of the aforementioned PayPal accounts, [redacted]. A cell phone number is "confirmed" when a user confirms receipt of an automated text message from PayPal by entering an alphanumeric code included in the text message. By using open source and FBI internal record searches, a number of documents associated Shariq HASHME with mobile number [redacted] and the aforementioned addresses.

22. In addition, PayPal records included banking information related to the ability of PayPal users to transfer money from their PayPal account to a debit/credit card or to another financial institution. The PayPal accounts registered to Bruno.Day.1988@outlook.com and dragonball844@outlook.com listed the following accounts:

Account # Status Name Start Date Expiration Date
[redacted] *2713 INACTIVE Bruno Day 6-Mar-19* [redacted]
Type Issuer Confirmed Issue# Currency
VISA CREDIT Bank of America-Consumer Credit Unconfirmed - USD
and
Account # Status Name Start Date Expiration Date
[redacted] *3421 INACTIVE Bruno Day 6-Mar-19* [redacted]
Type Issuer Confirmed Issue# Currency
VISA PREPAID Central Bank of Kansas City Unconfirmed – USD
and
Account # Status Name Start Date Expiration Date
[redacted] *9824 ACTIVE Bruno Day 6-Mar-19* [redacted]
Type Issuer Confirmed Issue# Currency
VISA DEBIT Bank of America, National Association Unconfirmed - USD
and
Account # Status Name Start Date Expiration Date
[redacted] *9824 ACTIVE Victor Montoya 24-Jun-19* [redacted]
Type Issuer Confirmed Issue# Currency
VISA DEBIT Bank of America, National Association Unconfirmed - USD

23. Additionally, during the records searches, personal email addresses of [redacted] and [redacted] for HASHME were revealed. The FBI obtained records from PayPal for an account registered to [redacted]. In part, PayPal records provided the subscriber information, IP logs and transaction history for the accounts registered to [redacted]. The subscriber information of the PayPal accounts included the following:

First Name: Shariq
Last Name: Hashme
DOB: [redacted]
Email: [redacted]
Address: [redacted] (Entered on 9/27/17)
Telephone: [redacted]
Time Created: July 30, 2011, 13:25:31
Bank Name: Bank of America
Bank Account: [redacted] 2236

24. Based on the PayPal records for the bruno.day.1988@outlook.com and [redacted] accounts, IP addresses geo-located in Thailand accessed both accounts during a time period relevant to the aforementioned cyber incidents. This approximate time period and location matched the previously-provided suspicious IP noted by Company A, also geo-located in Thailand, which connected to its internal payment database on April 30, 2019. The records below reflect a portion of relevant IP address logs:

Date/Time (PST/PDT)	IP Address	PayPal Account	ISP	Location
05 May 2019 21:05:33	182.232.145.215	[redacted]	TH_AIS_Mobile Internet	Bangkok, Thailand
05 May 2019 3:53:19	182.232.145.215		TH_AIS_Mobile Internet	Bangkok, Thailand
04 May 2019 22:12:08	182.232.145.215		TH_AIS_Mobile Internet	Bangkok, Thailand
04 May 2019 4:24:39	182.232.161.90		TH_AIS_Mobile Internet	Bangkok, Thailand
04 May 2019 1:07:22	182.232.161.90		TH_AIS_Mobile Internet	Bangkok, Thailand
03 May 2019	182.232.161.90		TH_AIS_Mobile	Bangkok,

Date/Time (PST/PDT)	IP Address	PayPal Account	ISP	Location
2:58:59			Internet	Thailand
03 May 2019 2:49:51	182.232.161.90	bruno.day.1988@outlook.com	TH_AIS_Mobile Internet	Bangkok, Thailand
02 May 2019 20:36:14	182.232.161.90	bruno.day.1988@outlook.com	TH_AIS_Mobile Internet	Bangkok, Thailand
02 May 2019 17:39:59	182.232.161.90	[redacted]	TH_AIS_Mobile Internet	Bangkok, Thailand
01 May 2019 20:54:35	182.232.194.57		TH_AIS_Mobile Internet	Bangkok, Thailand
01 May 2019 17:43:09	182.232.194.57		TH_AIS_Mobile Internet	Bangkok, Thailand
01 May 2019 5:00:09	182.232.194.57		TH_AIS_Mobile Internet	Bangkok, Thailand
01 May 2019 3:12:37	182.232.191.33		TH_AIS_Mobile Internet	Bangkok, Thailand

25. The FBI requested records associated with two bank accounts listed with the PayPal accounts registered to Bruno.Day.1988@outlook.com and dragonball844@outlook.com ([redacted]2713 and [redacted]9824), "Bruno Day," and "Shariq Hashme" from the issuing bank, Bank of America. In part, the records provided by Bank of America included the following information:

Account Number: [redacted]*2236*
Account Name: Shariq S Hashme
Address: [redacted]

26. The Bank of America records were linked by account owner information and direct deposits described below. The following transactions were observed in the transaction history portion of the Bank of America records for account [redacted]2236, an account linked to the PayPal account registered to [redacted], which mirrors PayPal withdrawals from the account registered to Bruno.day.1988@outlook.com:

Date	Amount	Payment Received From	City, State
June 7, 2019	$3,009.50	PayPal *Day Bruno	San Jose, CA
May 31, 2019	$3,009.50	PayPal *Day Bruno	San Jose, CA

Date	Amount	Payment Received From	City, State
May 24, 2019	$3,009.50	PayPal *Day Bruno	San Jose, CA
May 10, 2019	$3,284.00	PayPal *Day Bruno	San Jose, CA
April 29, 2019	$3,146.75	PayPal *Day Bruno	San Jose, CA
April 19, 2019	$3,146.75	PayPal *Day Bruno	San Jose, CA
April 12, 2019	$3,274.15	PayPal *Day Bruno	San Jose, CA
March 22, 2019	$951.14	PayPal *Day Bruno	San Jose, CA
March 15, 2019	$533.79	PayPal *Day Bruno	San Jose, CA
March 8, 2019	$1,044.88	PayPal *Day Bruno	San Jose, CA
March 6, 2019	$23.63	PayPal *Day Bruno	San Jose, CA
March 6, 2019	$336.15	PayPal *Day Bruno	San Jose, CA

27. The FBI collected additional information on the subject, Shariq HASHME, from California DMV records. The following identifiers relate to HASHME:

DL Number: [redacted]
Name: Shariq S. Hashme
DOB: [redacted]
Address: [redacted]
Sex - M; **Hair** - Black; **Eyes** - Brown; **Height** - 5'11"; **Weight** – 160

28. According to one of HASHME's social media profiles, he was most recently employed as an engineer at Company A and located in San Francisco, California. HASHME is a citizen of the United Kingdom and is believed to have left the United States to live overseas on April 18, 2019, due to an expired work visa.

29. Company A advised that at no time during the aforementioned cyber incidents was HASHME authorized to access or alter the data or contents of the internal payment database, or cause the aforementioned rewards payments to be made to himself.

30. Furthermore, Company A informed the FBI that an internal investigation revealed the destruction of payment database logs. Specifically, shortly after HASHME accessed internal Company A infrastructure via his Virtual Private Network (VPN), database logs were altered to delete the record of some of the fraudulent payments sent to the PayPal account registered to

Bruno.Day.1988@outlook.com, an account controlled by HASHME.

Discovery of HASHME Arrival

31. On August 7, 2019, the FBI received information that HASHME was expected to return to the United States by way of San Francisco International Airport on or about August 9, 2019. The FBI received additional information on August 9, 2019 that HASHME is expected to return to the United States by way of SFO the next day, on August 10, 2019.

CONCLUSION

32. Based on the evidence uncovered and the information provided by Company A as well as records received by the FBI, it is believed that HASHME connected to Company A's internal payment servers to alter and divert bonus payments that were ultimately deposited to a bank account he owned and controlled, resulting in losses of at least approximately $40,000. Furthermore, as advised by Company A, HASHME had no authorization, legitimate business requirements, or need, to access or alter payment information in Company A's internal payment database. I respectfully submit that there is probable cause to believe that HASHME knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and thereby caused loss to one or more persons during a one-year period affecting protected computers aggregating at least $5,000 in value, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i), and (c)(4)(A)(i)(I).

REQUEST FOR SEALING

33. Because this investigation is continuing, disclosure of the arrest warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of the arrest warrant at this time would seriously jeopardize the

investigation; as such a disclosure would allow HASHME to change patterns of behavior, notify other confederates, destroy evidence, or flee or continue flight from prosecution. Accordingly, I request that the Court issue an order that the complaint, arrest warrant, this affidavit in support of application for complaint and arrest warrant, and all attachments thereto be filed under seal until further order of this Court.

ROBBIE J. ROBERTSTON
Special Agent
Federal Bureau of Investigation

Sworn to before me this ____ day of August 2019

HONORABLE ELIZABETH D. LAPORTE
United States Magistrate Judge